

# AdaCore DIGEST

JULY 2024



## 24.2 Release

We're happy to announce the release of the second stable version of our technology, GNAT Pro 24.2. This is the bugfix version of branch 24 that we recommend for production builds and the last release for enterprise customers. After that point, subscribers to GNAT Pro Assurance products will still be eligible for critical bugfix releases on the 24 branch. [Full release notes are available here.](#)

Starting with this 24.2 release, you can download the vulnerability report for each product from the "Release Download" section of GNAT Tracker. It will provide you with a list of the CVEs that can impact this product and the corresponding impact analysis describing whether the product is affected by each CVE.

## Fuzzing with GNATfuzz

With the introduction of GNAT Pro release 24, GNATfuzz now incorporates a highly efficient input-to-state correspondence capability, known as CMPLOG. This feature significantly enhances the dynamic path-solving logic of the fuzzer. CMPLOG is designed to analyze potential relationships between a subprogram's input space (parameters) and constant values used within comparison instructions on branch conditions within the subprogram control flow. When CMPLOG identifies a strong relationship, test cases that can solve the associated branch conditions are generated, freeing up mutation cycles to focus on solving other, more complex branch conditions.

For example, in the code below, the newly integrated CMPLOG feature would quickly determine that solving the branch condition is achieved by generating a test case with the value 10\_000.

```
Unset
procedure Demonstration (Parameter : Integer) is
begin
  if Parameter = 10_000 then
    Put_Line ("Branch entered!");
  end if;
end Demonstration;
```



Another significant update in release 24 is the enhanced integration with GNATtest. This integration, now more robust, is facilitated through a standard test case format. The collaborative nature of this integration is a key highlight, as it allows GNATtest and GNATfuzz to share results. This mutually beneficial feature ensures that GNATtest can contribute to a GNATfuzz starting corpus and that GNATfuzz can generate additional test cases that further the coverage achieved through a GNATtest campaign.

For GNAT Pro release 25, AdaCore engineering is working on completely refactoring the "fuzz" mode phase. This exercise aims to create an abstraction layer between GNATfuzz and the existing AFL++ fuzzer and implement a generic fuzzer API so that GNATfuzz can support multiple fuzzer backends. Furthermore, the first candidate identified is LibFuzzer. LibFuzzer is a widely used open-source LLVM-based tool that will enhance GNATfuzz results and allow us to support fuzzing campaigns on native Microsoft Windows.

Also planned for the GNAT Pro 25 release is GNATfuzz for C. Fuzz testing C applications and quickly flushing out memory-related vulnerabilities like buffer overflows is something multiple customers have requested. This capability will involve directly fuzzing C functions via a new test harness generation feature.

Finally, GNATfuzz will supplement the CMPLOG feature integrated within GNAT Pro release 24 with a Symbolic Execution capability through an integration with the open-source tool SymCC. CMPLOG is exceptional at quickly solving tight branches where there is an input-to-state correspondence. However, SymCC goes much further and dynamically computes symbolic expressions for each value in the program and then utilizes theorem provers to solve complex branch conditions and generate test cases that provide broad coverage of the code under test.

## Events

### AdaCore Tech Day in Paris

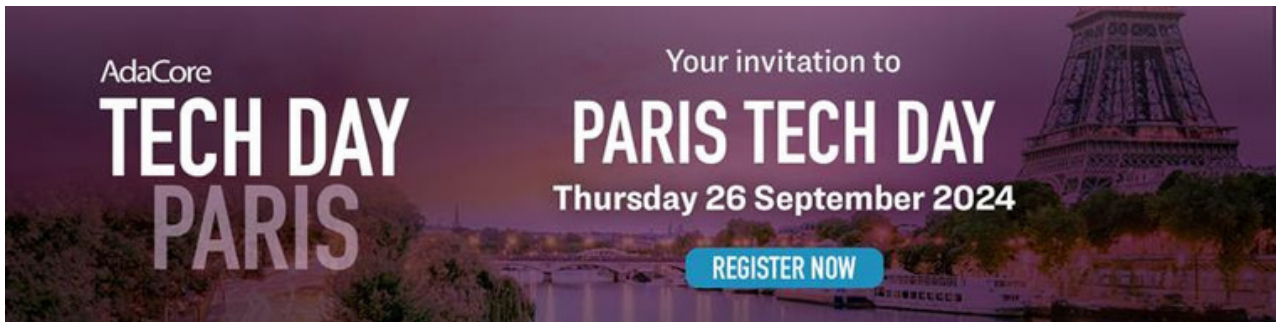
AdaCore Tech Days are back! Join us in Paris on Thursday, September 26th, to learn about the latest advancements in high-integrity software from AdaCore experts.

The registration deadline has been extended to 2nd August. [Register now to secure your place](#)

What's on the agenda:

- AdaCore strategy and technical roadmap
- High integrity software development
- Static and dynamic analysis
- Cybersecurity
- Programming Languages (Ada, C, C++, SPARK, Rust)
- Artificial Intelligence in Development Tools and DevOps
- Demos and workshops on cutting-edge tech from AdaCore experts
- Networking with the critical software community

[Register for Paris Tech Day](#)



### **Farnborough International Airshow**

AdaCore will be attending the Farnborough International Airshow 2024, which will host leading innovators from the aerospace, aviation and defence industries and beyond: [more info about the Airshow](#).

## **Training**

Transform your programming skills with our Public Ada Virtual Training Course. This standardized course is perfect for individuals and small groups who want to master the Ada language when private, customized training is not a feasible option. Over five days, you'll dive into the core features of Ada through instructor-led lectures, participatory quizzes, and hands-on lab exercises.

Our curriculum covers essential programming concepts and advanced Ada language features. This course is suitable for those with a software engineering background or experience in any compilable programming language.

Join us remotely for an immersive learning experience that will enhance your proficiency in Ada. Upcoming dates are available in both the EU and the US:

#### US Public Ada Training:

- September 16 - 20, 2024
- March 17 - 21, 2025
- September 8 - 12, 2025

#### EU Public Ada Training:

- January 6 - 10, 2025
- June 16 - 20, 2025

[Register now to secure your spot](#) and elevate your programming capabilities.

## CHERI Booklet

Our new digital booklet provides deeper insights into GNAT Pro for CHERI and how this solution enhances memory safety in modern systems and eradicates many memory-related vulnerabilities.

GNAT Pro for CHERI also provides a complete Ada toolchain to build secure applications executing on Arm Morello, a Capability Hardware Enhanced RISC Instructions (CHERI) CPU. Enhancements to the GNAT Pro GCC and LLVM bare-metal Ada runtimes bring automated CHERI pure-capability memory allocators and other novel security features to the developer, permitting new security-by-design paradigms to systems development.

[Learn more about GNAT Pro for CHERI](#)

## Security Considerations in Light Launcher Software

At AdaCore, we understand the crucial role of secure software in space industry projects. Selecting the right programming languages and development tools is foundational to building safe and reliable systems. We focus on memory-safe languages and formal verification to enhance security measures in software development. Memory-safe languages prevent common vulnerabilities such as buffer overflows, while formal verification proves the correctness of software against its specifications.

These practices not only increase the security of software but also ensure compliance with industry standards and regulatory requirements. Our approach has been successfully applied in projects like the Zephyr satellite launcher, where high-integrity software solutions have significantly contributed to the project's anticipated success and security. [Read more.](#)

## Creating Your Own Ada/SPARK Coding Standard

In our blog post, we introduce a new initiative to help users create their own Ada/SPARK coding standards using GNATcheck. Recognizing the demand for a simpler setup process, we've developed a baseline coding standard that users can adopt or adapt according to their project needs. This standard, which includes guidelines for good programming practices and code consistency, is complemented by GNATcheck, allowing for automated enforcement and enhanced code quality assurance.

You can explore the full details of how to implement and customize your coding standard [here](#).

## AdaCore in the press

### Battery Ventures Teams with AdaCore for High Integrity Software Development

“Battery Ventures is investing in AdaCore which will realize AdaCore's expansion, placing the company as a go-to source for high-integrity software-development tooling.”

*Featured in Embedded Computing Design*

### Why Commercial Rust Software is Critical for Critical Solutions

“Rust is a programming language that's growing in popularity because of its safety features, particularly its memory tracking aspects (take our Quick Poll below about your Rust usage). It can address high-level applications as well as low-level programs such as device drivers. Rust is one of the few languages that can be used to deliver Linux device drivers.”

*Featured in Electronic Design*

### AdaCore Research Proves Novel Solution for 'Security by Default'

“In an age of increasing security breaches and cyberattacks, the need for robust and comprehensive security mechanisms within embedded real-time systems is paramount. Through its research, AdaCore has demonstrated how combining memory-safe hardware with memory-safe software results in a mutualistic layered approach to security and increases the assurance of embedded real-time systems.”

*Featured in Military Systems Technology*

If you have questions about any of the technologies or services mentioned above, please reach out to your Account Manager or email us at [info@adacore.com](mailto:info@adacore.com)